Configuration de l'administration des périphériques TACACS+ sur Palo Alto avec ISE

Table des matières

Introduction

Conditions préalables

Composants utilisés

Diagramme du réseau

- Flux d'authentification

Configurer

- Section 1 : Configuration du pare-feu Palo Alto pour TACACS+
- Section 2 :Configuration de TACACS+ sur ISE

Vérifier

- Évaluation ISE

Dépannage

- 1 TACACS : Paquet de demande TACACS+ non valide - Secrets partagés éventuellement incorrects
  - Problème
  - Causes possibles
  - Solution
- 2.No ISE TACACS Live Log

Introduction

Ce document décrit la configuration TACACS+ sur Palo Alto avec Cisco ISE.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE et le protocole TACACS+.
- Pare-feu Palo Alto.

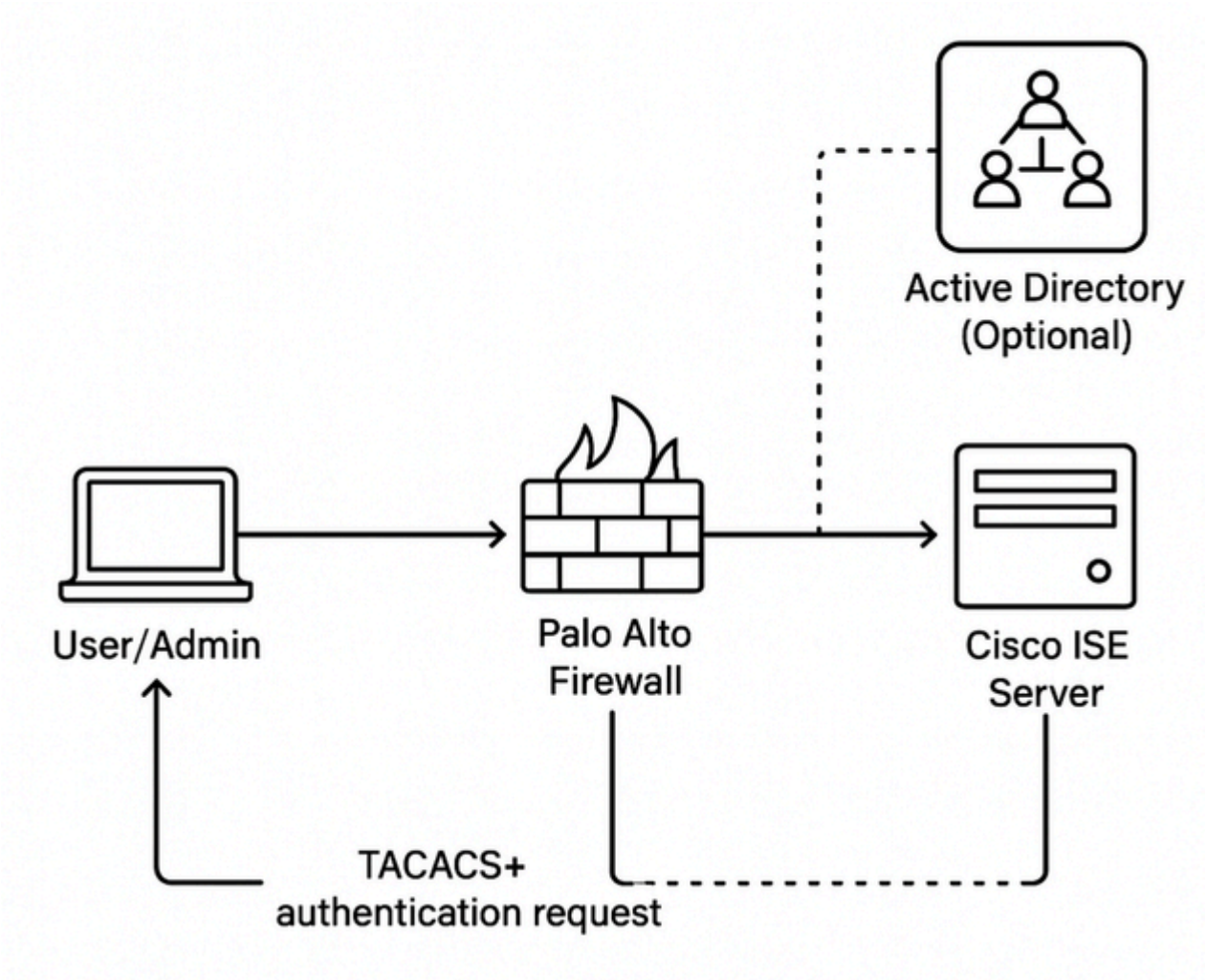
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Palo Alto Firewall version 10.1.0
- Cisco Identity Services Engine (ISE) version 3.3 Patch 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme du réseau



Flux d'authentification

1. L'administrateur se connecte au pare-feu Palo Alto.

2. Palo Alto envoie une demande d'authentification TACACS+ à Cisco ISE.

3. Cisco ISE :

- Si AD est intégré, il interroge AD pour l'authentification et l'autorisation.
- En l'absence d'Active Directory, il utilise des stratégies ou des magasins d'identités locaux.
- Cisco ISE envoie une réponse d'autorisation à Palo Alto en fonction des stratégies configurées.
- L'administrateur obtient l'accès avec le niveau de privilège approprié.

Configurer

Section 1 : configuration du pare-feu Palo Alto pour TACACS+

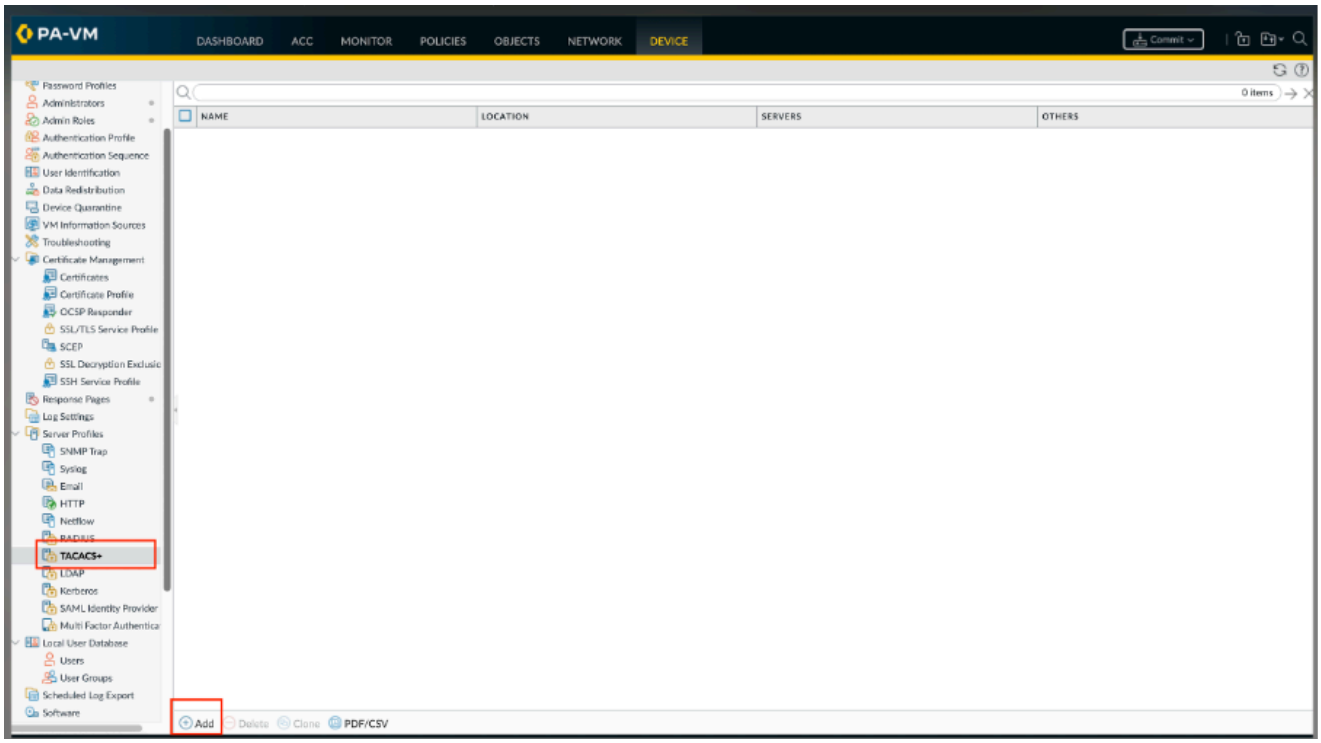
Étape 1 : ajout d’un profil de serveur TACACS+

Le profil définit comment le pare-feu se connecte au serveur TACACS+.

1. Sélectionnez Device > Server Profiles > TACACS+ or Panorama > Server Profiles > TACACS+ on Panorama et Add a profile.
2. Entrez un nom de profil pour identifier le profil de serveur.
3. (Facultatif) Sélectionnez Administrator Use Only pour limiter l'accès aux administrateurs.
4. Entrez un délai d'attente en secondes après lequel une demande d'authentification expire (la valeur par défaut est 3 ; est comprise entre 1 et 20).
5. Sélectionnez le protocole d'authentification (CHAP par défaut) que le pare-feu utilise pour s'authentifier auprès du serveur TACACS+.

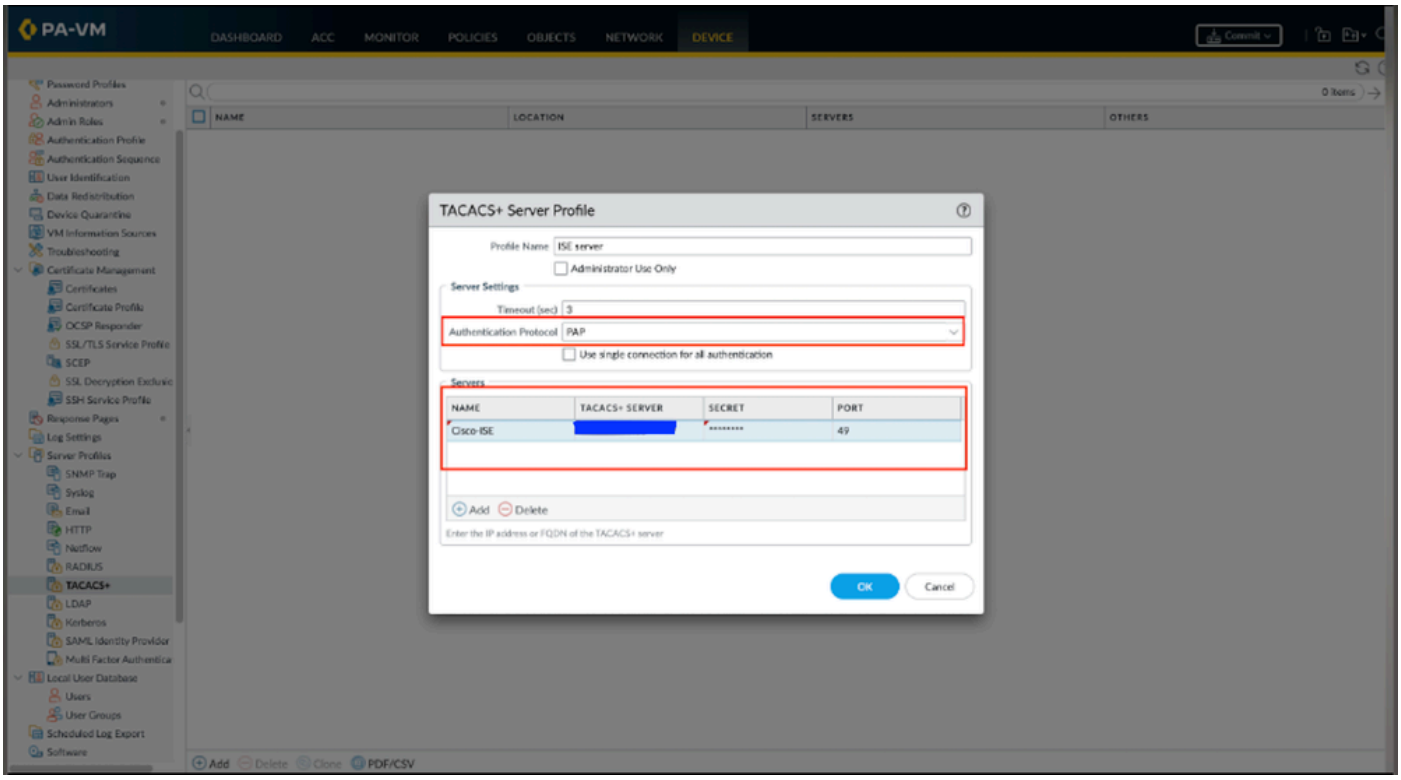
Le protocole d'authentification TACACS+ par défaut de Palo Alto est CHAP (CHAP/MD5).

Lorsque ISE authentifie les utilisateurs par rapport à un magasin d'identités externe tel qu'Active Directory, CHAP/MD5 ne peut pas être utilisé car AD ne fournit pas à ISE les informations de mot de passe réversibles requises pour la validation CHAP. Par conséquent, pour l'authentification soutenue par AD, configurez le profil de serveur Palo Alto TACACS+ pour utiliser PAP, et non CHAP

1. 

2. Ajoutez chaque serveur TACACS+ et procédez comme suit :
    1. Un nom pour identifier le serveur.
    2. Adresse IP ou nom de domaine complet du serveur TACACS+. Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et que vous modifiez ensuite l'adresse, vous devez valider la modification pour que la nouvelle adresse de serveur prenne effet.
    3. Secret et Confirm Secret pour chiffrer les noms d'utilisateur et les mots de passe.
    4. Port du serveur pour les demandes d'authentification (49 par défaut). Cliquez sur OK pour enregistrer le profil de serveur.

7. Cliquez sur OK pour enregistrer le profil de serveur.



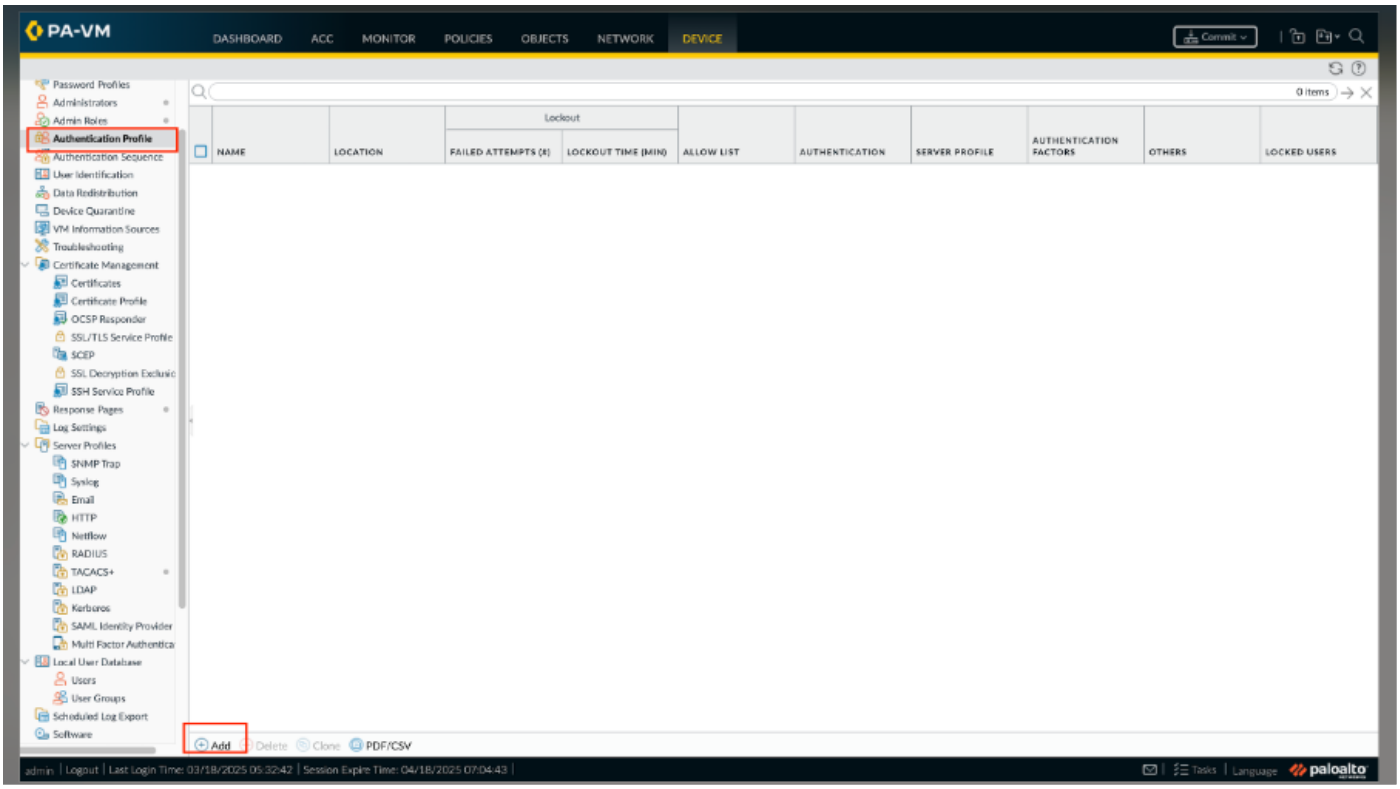
Conseil : Sélectionnez PAP lorsque vous utilisez Active Directory ou un autre magasin d'identités externe.

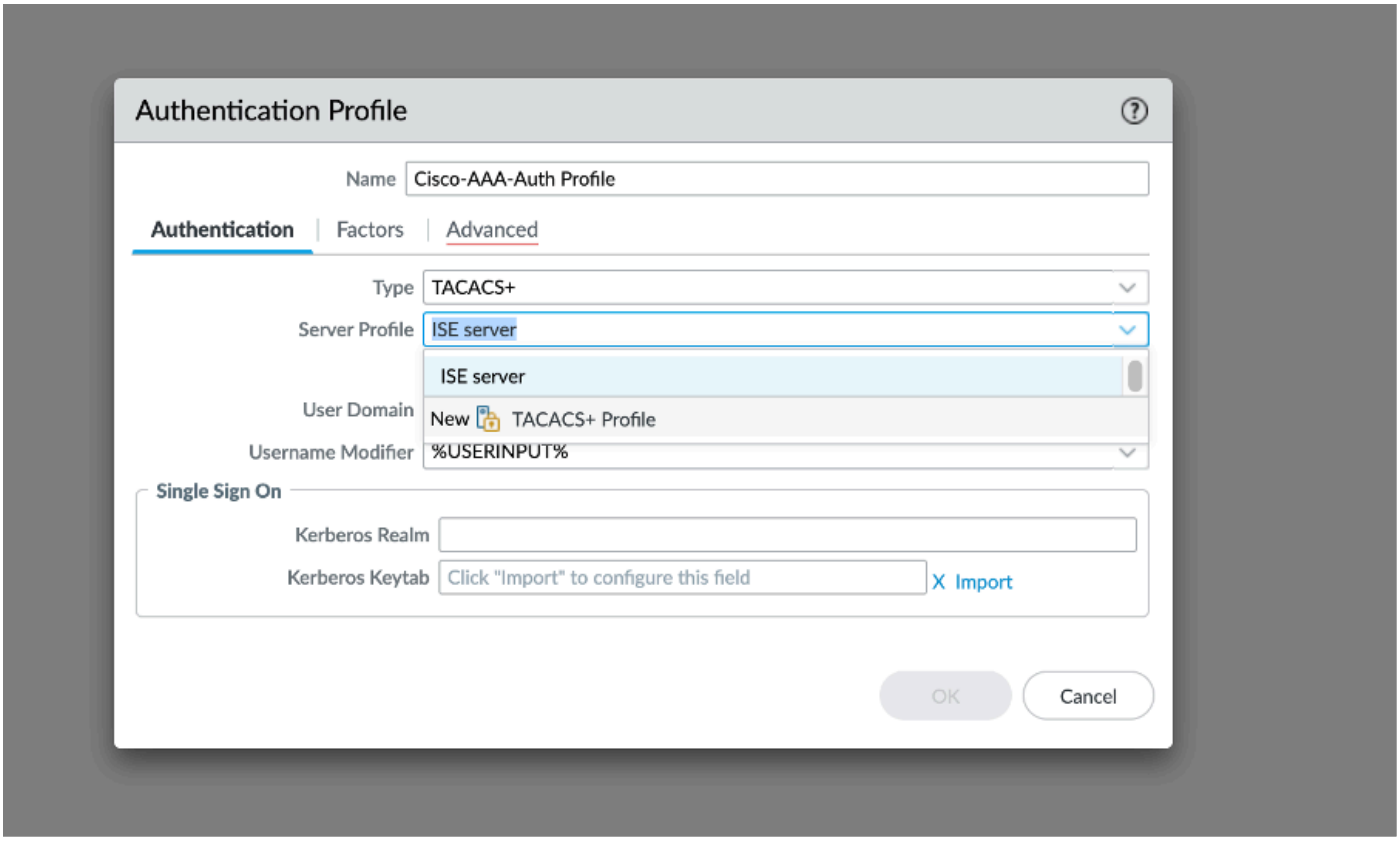
L'option CHAP de Palo Alto utilise CHAP/MD5. Cisco ISE ne peut pas valider les informations d'identification CHAP/MD5 par rapport à Active Directory, car Active Directory n'expose pas le contenu du mot de passe requis. Utilisez PAP pour l'authentification de l'administrateur TACACS+ soutenue par AD. Le protocole CHAP ne peut être utilisé que si la source d'identité ISE sélectionnée le prend en charge (par exemple, des utilisateurs internes correctement configurés).

Étape 2. Attribution du profil de serveur TACACS+ à un profil d’authentification

Le profil d'authentification définit les paramètres d'authentification communs à un ensemble d'utilisateurs.

1. Sélectionnez Device > Authentication Profile et Add a profile.
    1. Entrez un nom pour identifier le profil
    2. Définissez le type sur TACACS+.
    3. Sélectionnez le profil de serveur que vous avez configuré.
    4. Sélectionnez Récupérer le groupe d'utilisateurs à partir de TACACS+ pour collecter des informations de groupe d'utilisateurs à partir des VSA définies sur le serveur TACACS+.

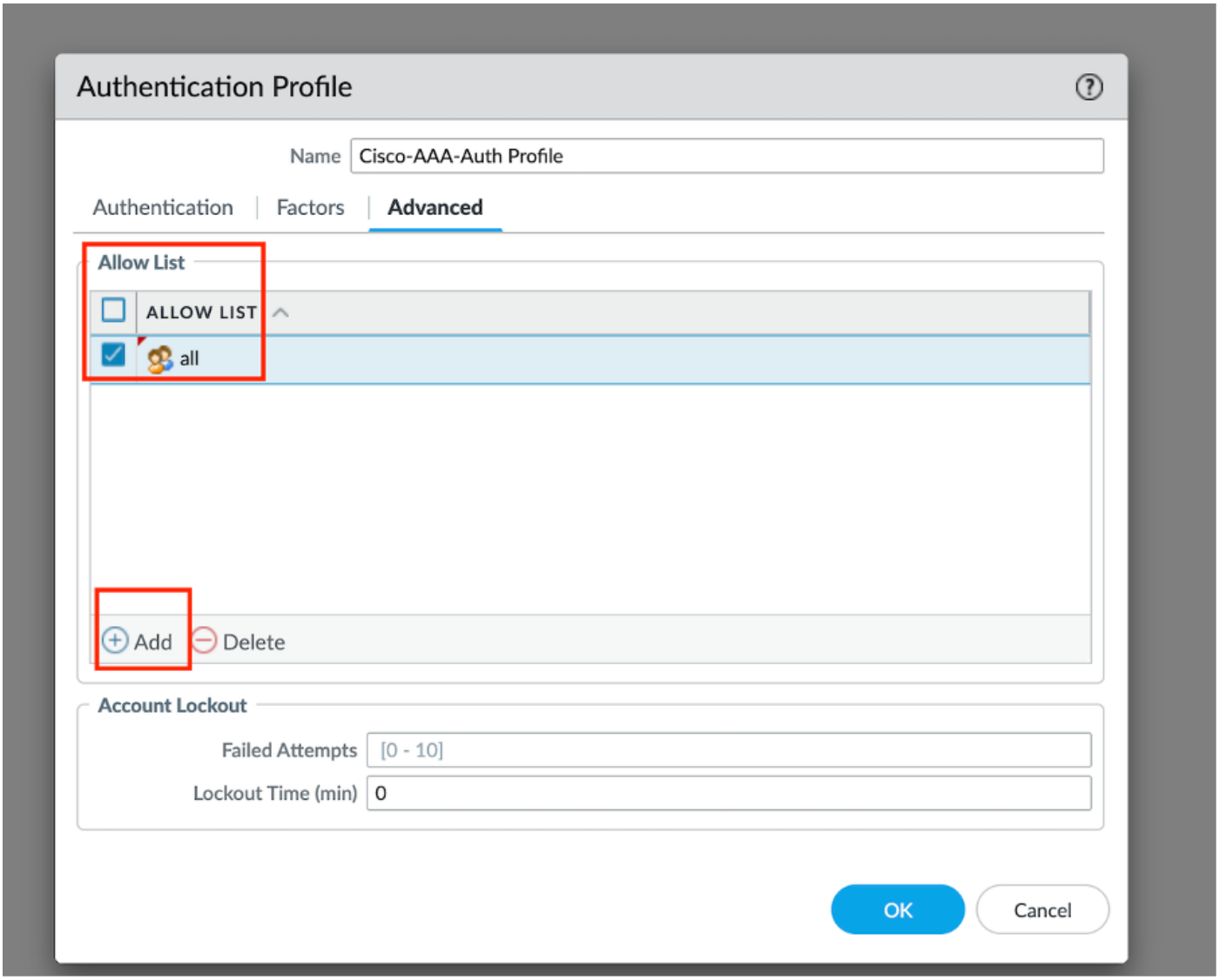




Le pare-feu fait correspondre les informations de groupe à l'aide des groupes que vous spécifiez dans la liste verte du profil d'authentification.

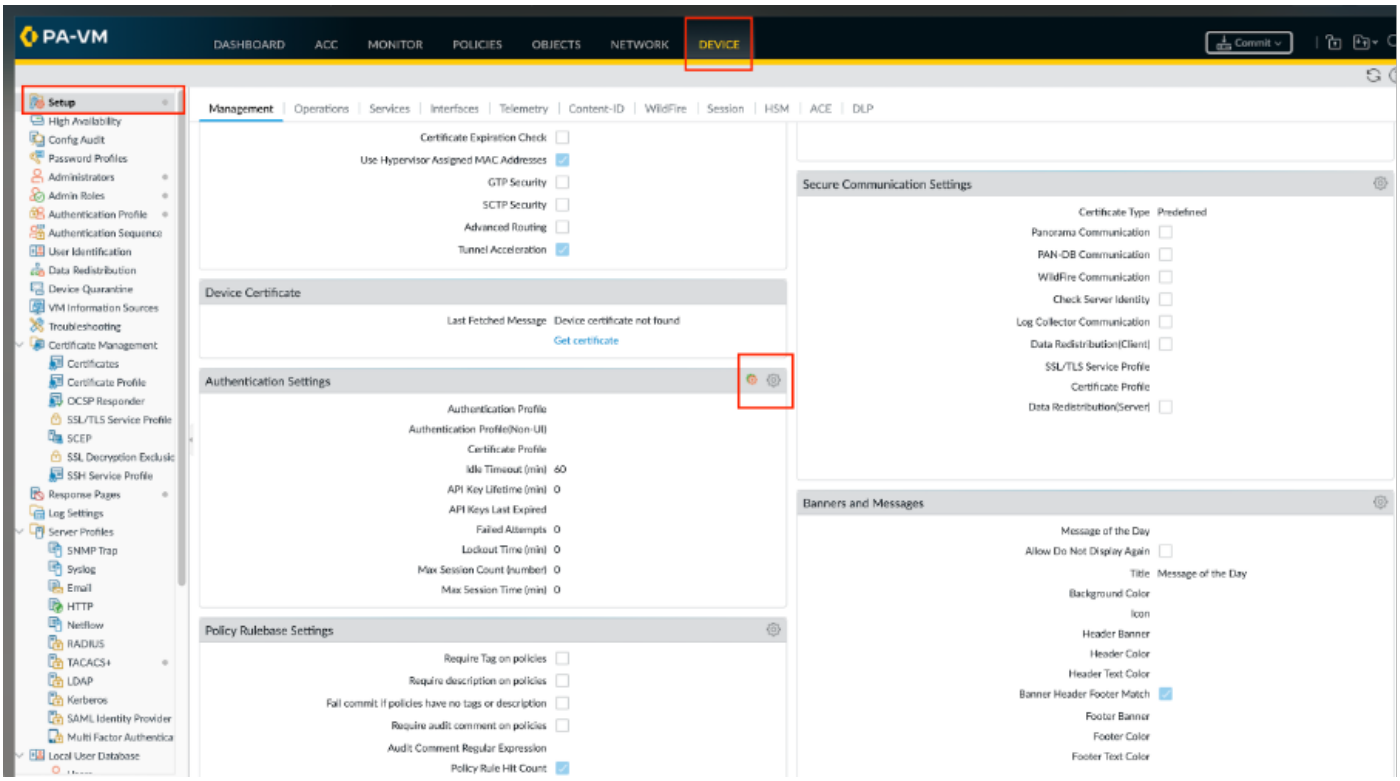
1. Sélectionnez Avancé et, dans la liste verte, Ajouter les utilisateurs et les groupes qui

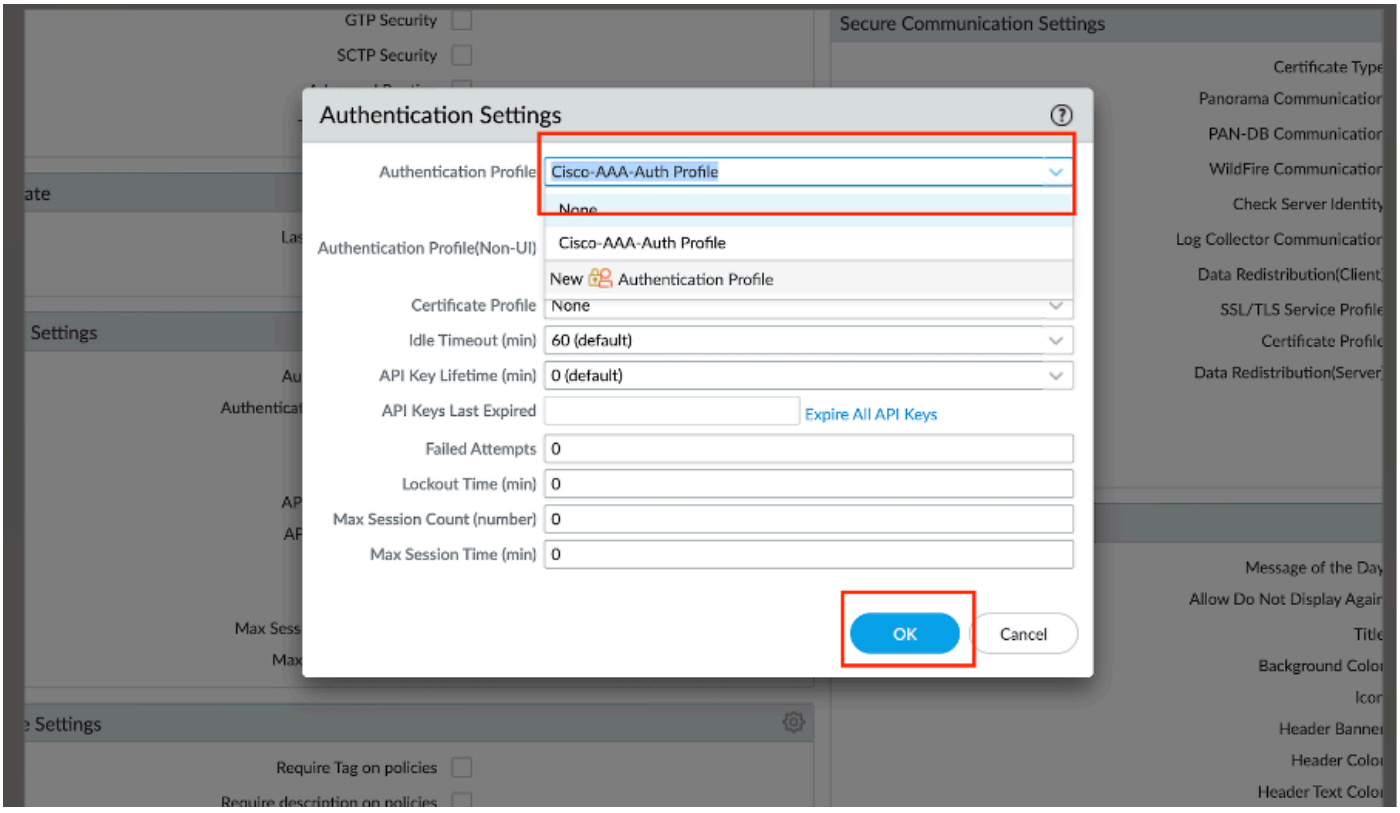
peuvent s'authentifier avec ce profil d'authentification.
2. Cliquez sur OK pour enregistrer le profil d'authentification.



Étape 3 : configuration du pare-feu pour utiliser le profil d’authentification pour tous les administrateurs

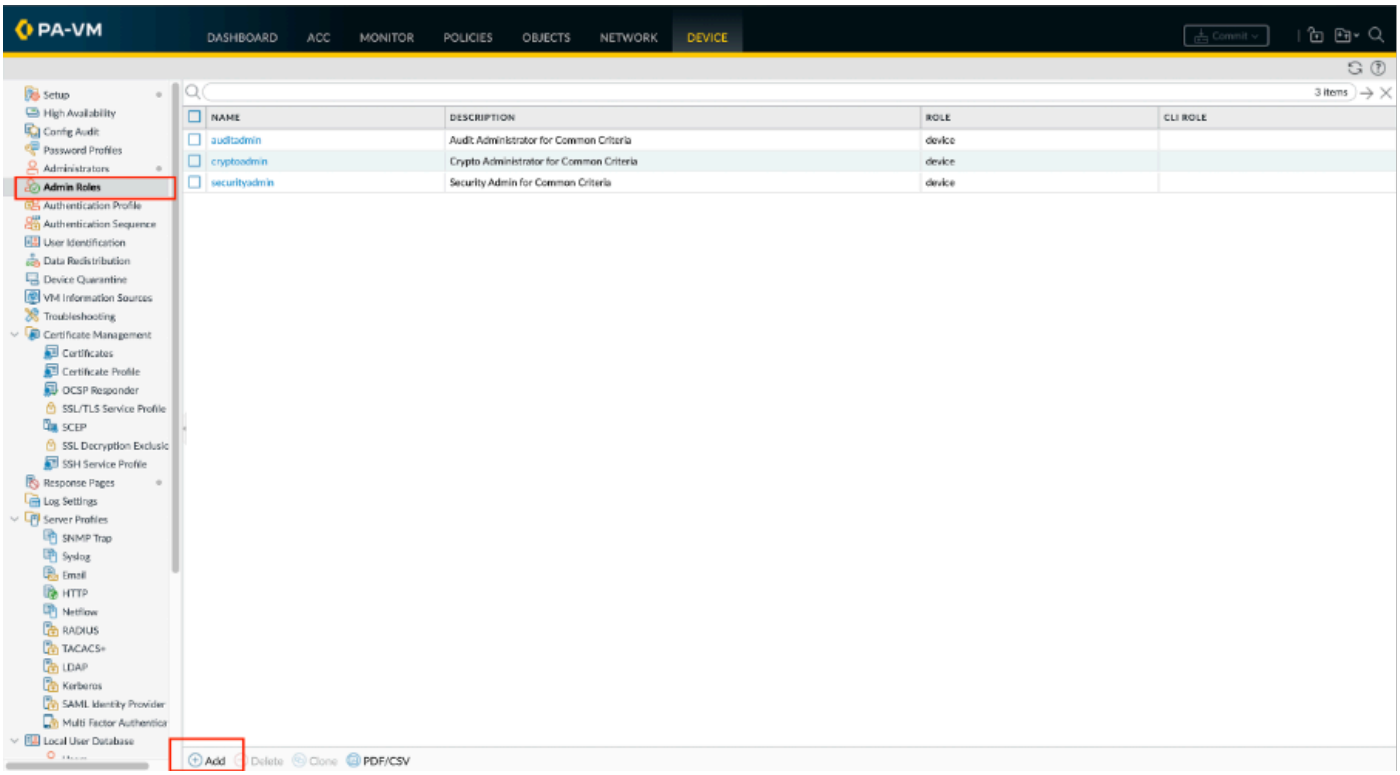
1. Sélectionnez Device > Setup > Management et modifiez les paramètres d'authentification.
2. Sélectionnez le profil d'authentification que vous avez configuré et cliquez sur OK.



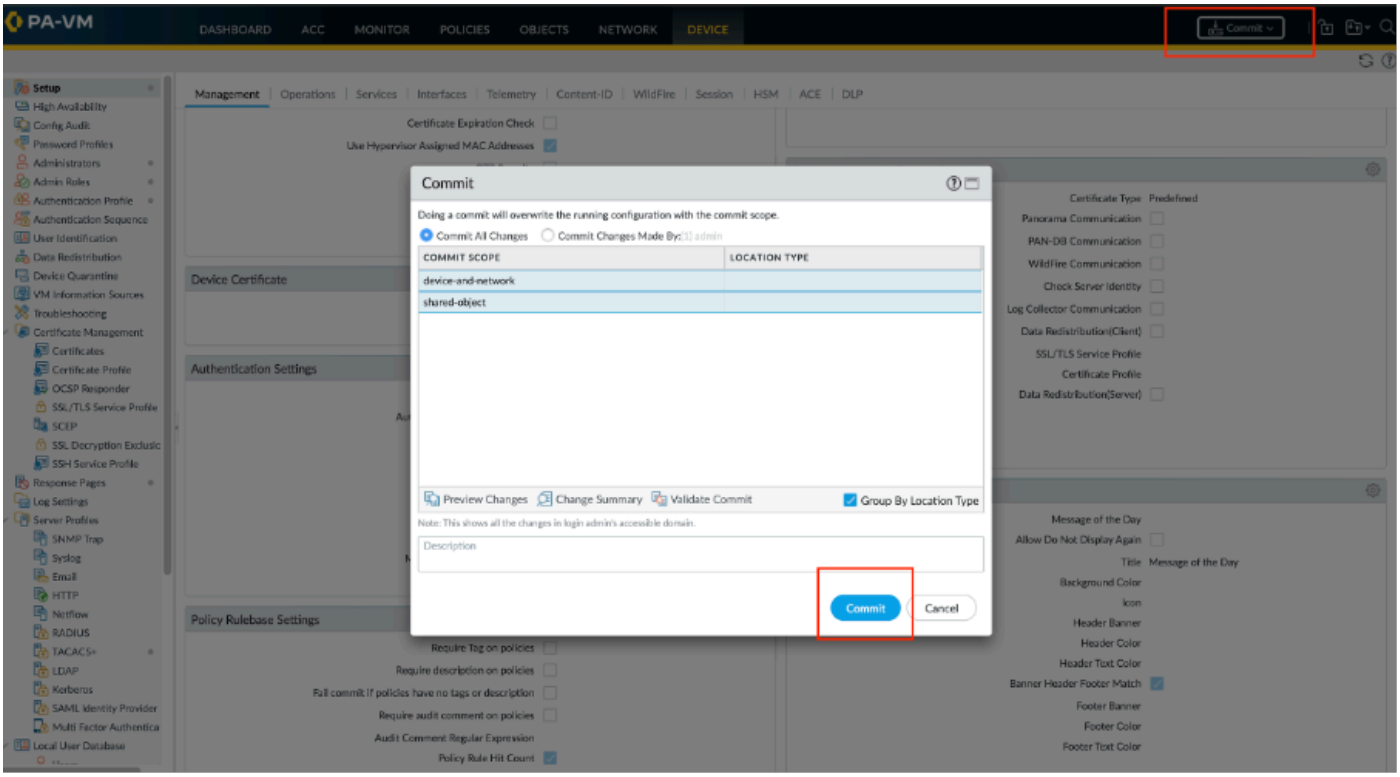


Étape 4 : configuration d’un profil de rôle admin

Sélectionnez Device > Admin Roles et cliquez sur Add. Entrez un nom pour identifier le rôle.



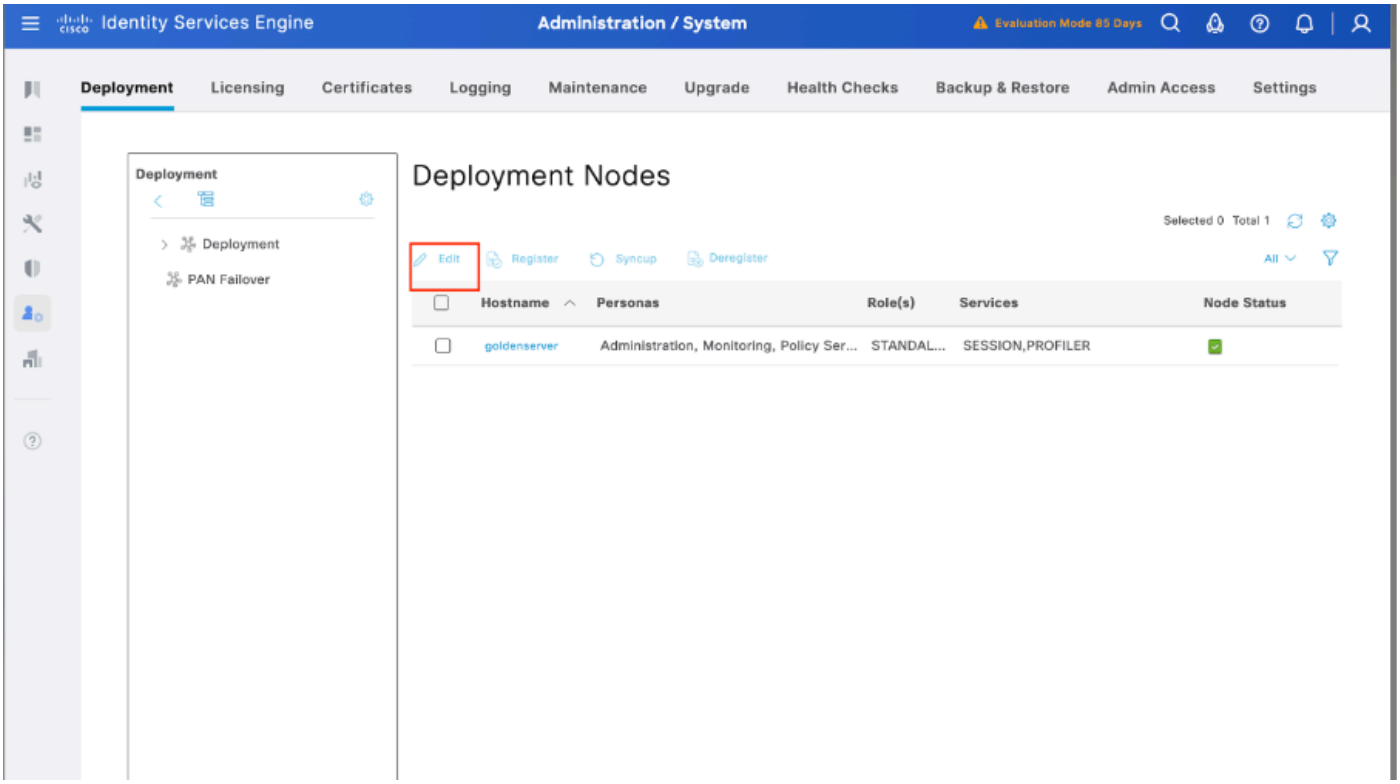
Étape 5. Validez vos modifications pour les activer sur le pare-feu.



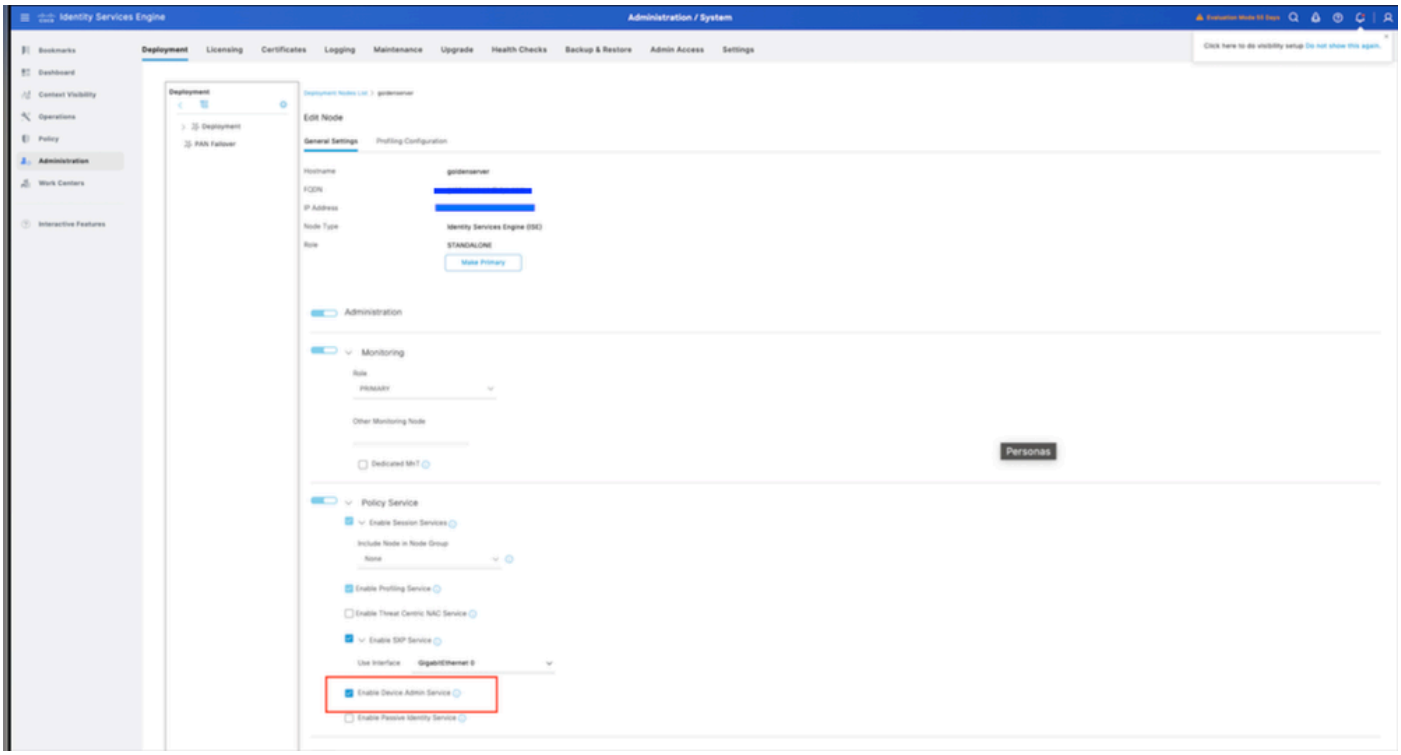
Section 2 : configuration de TACACS+ sur ISE

Étape 1. L'étape initiale consiste à vérifier si Cisco ISE dispose des capacités nécessaires pour

gérer l’authentification TACACS+. Pour ce faire, vérifiez que la fonctionnalité Device Admin Service est activée sur le noeud Service de stratégie (PSN) souhaité. Accédez à Administration > System > Deployment, sélectionnez le noeud approprié où ISE traite l'authentification TACACS+, et cliquez sur Edit pour revoir sa configuration.

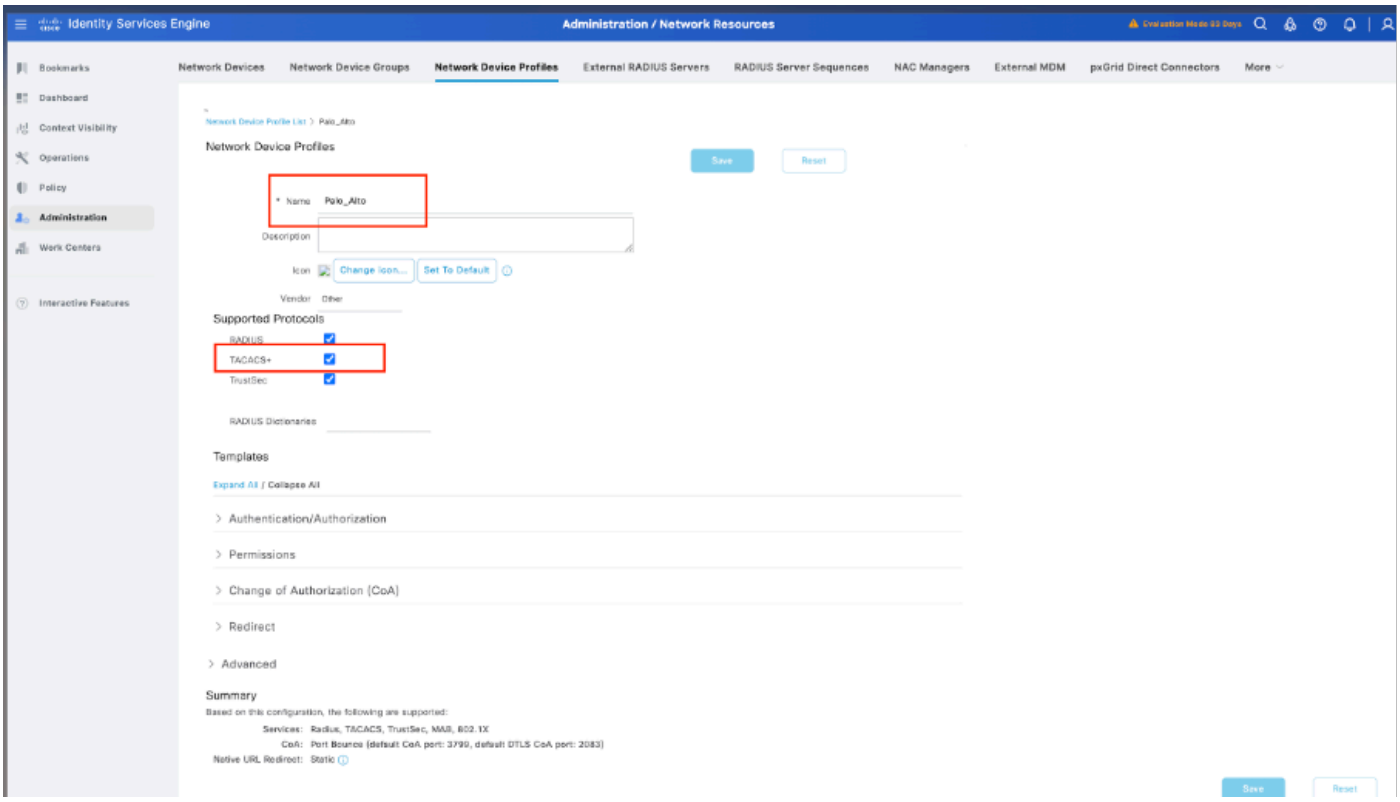


Étape 2. Faites défiler la page vers le bas pour localiser la fonction Device Administration Service. Notez que l'activation de cette fonctionnalité nécessite que le personnel Policy Service soit actif sur le noeud, ainsi que les licences TACACS+ disponibles dans le déploiement. Cochez la case pour activer la fonction, puis enregistrez la configuration.



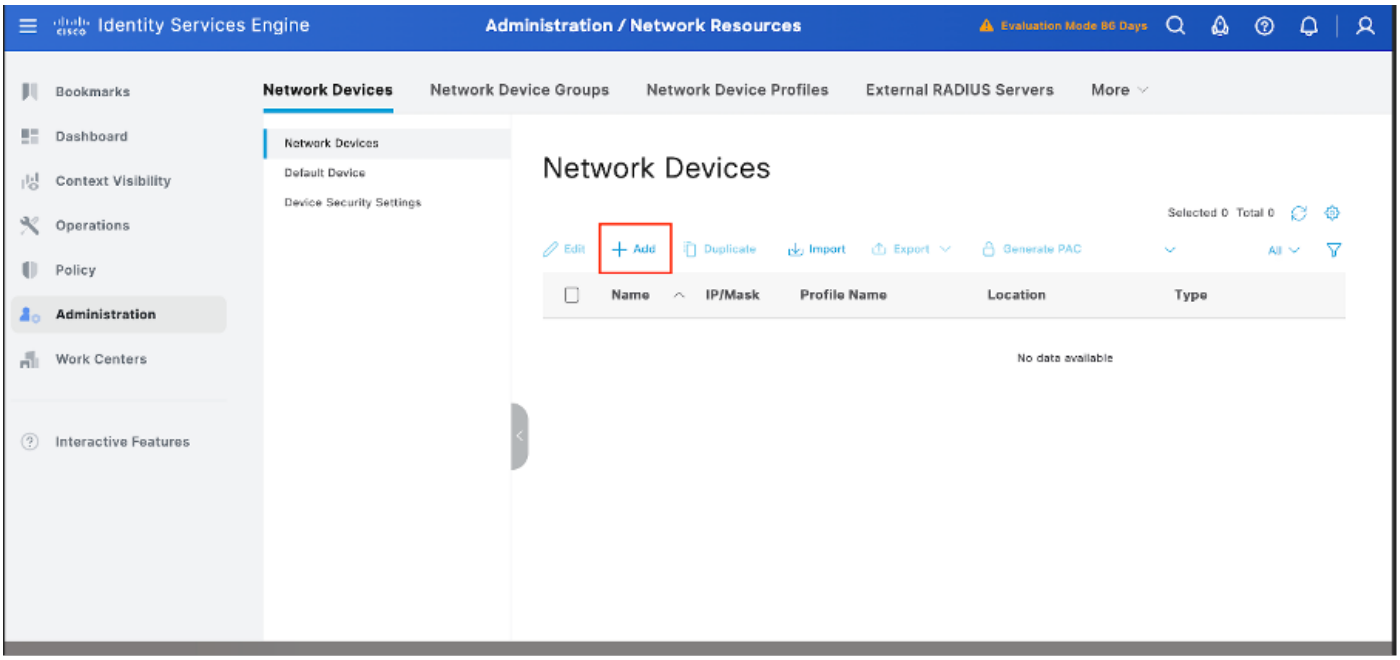
Étape 3 : configuration du profil de périphérique réseau Palo Alto pour Cisco ISE

Accédez à Administration > Network Resources > Network device profile. Cliquez sur Add et mentionnez le nom (Palo Alto) et activez TACACS+ sous les protocoles pris en charge.



Étape 4. Ajout de Palo Alto comme périphérique réseau

1. Accédez à Administration > Network Resources > Network Devices > +Add.



2. Cliquez sur Ajouter et entrez les informations suivantes :

Name : Palo-Alto

Adresse IP: <IP Palo-Alto>

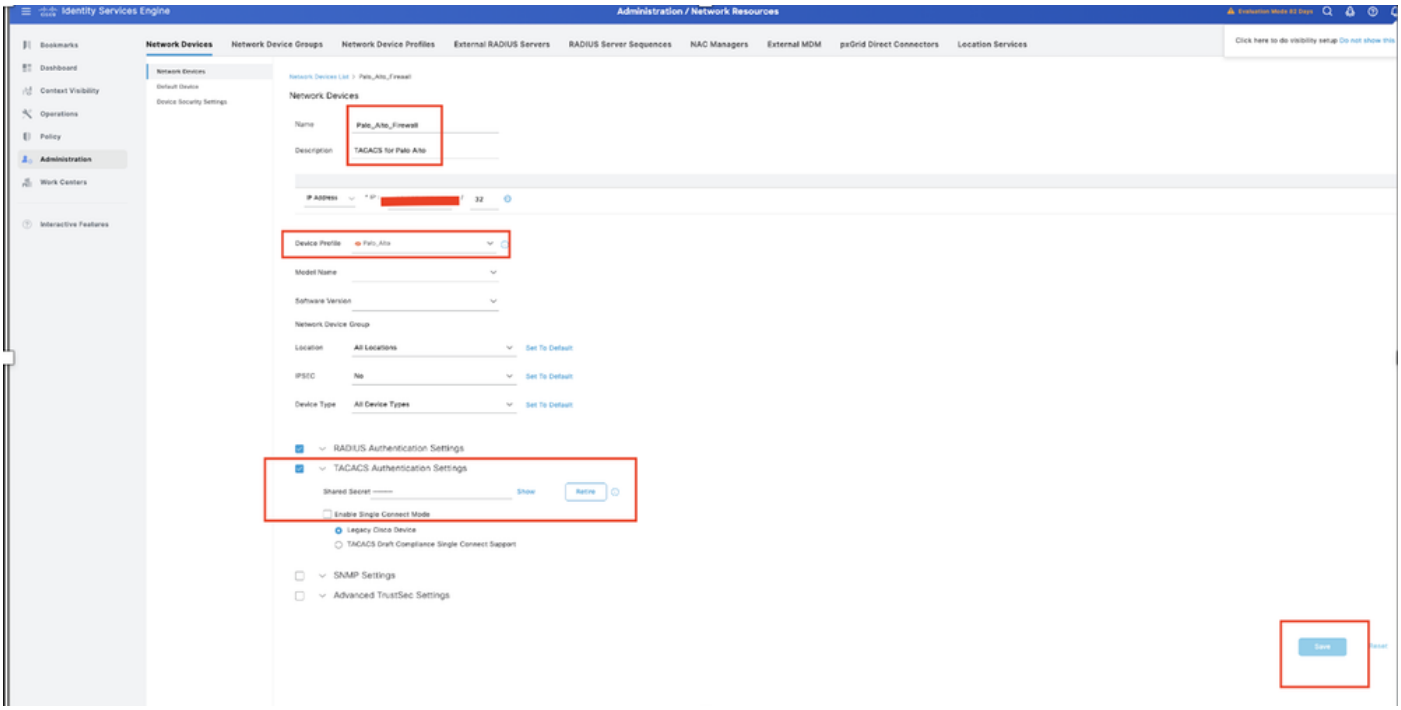
Profil de périphérique réseau : sélectionnez Palo Alto

Paramètres d'authentification TACACS :

Activer l'authentification TACACS+

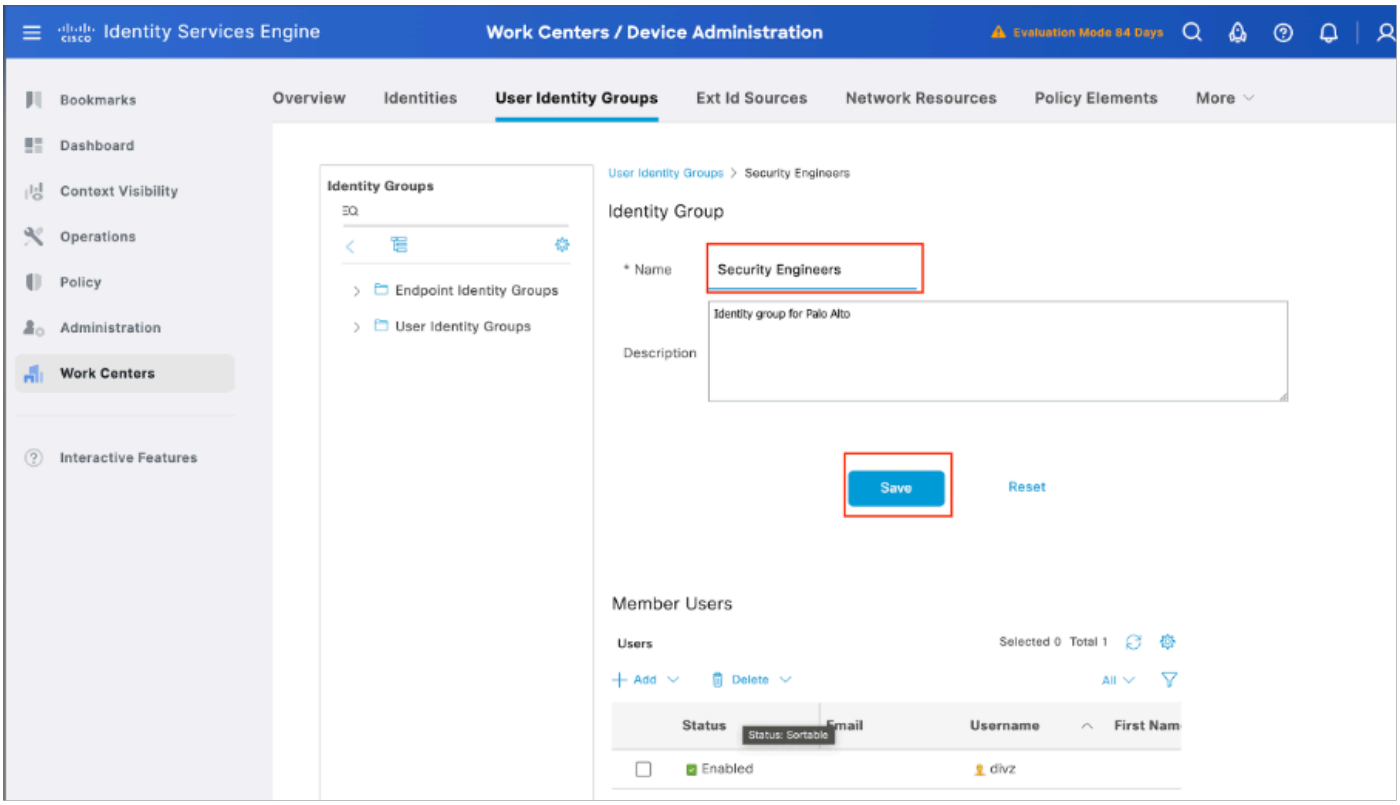
Saisissez le secret partagé (doit correspondre à la configuration Palo Alto)

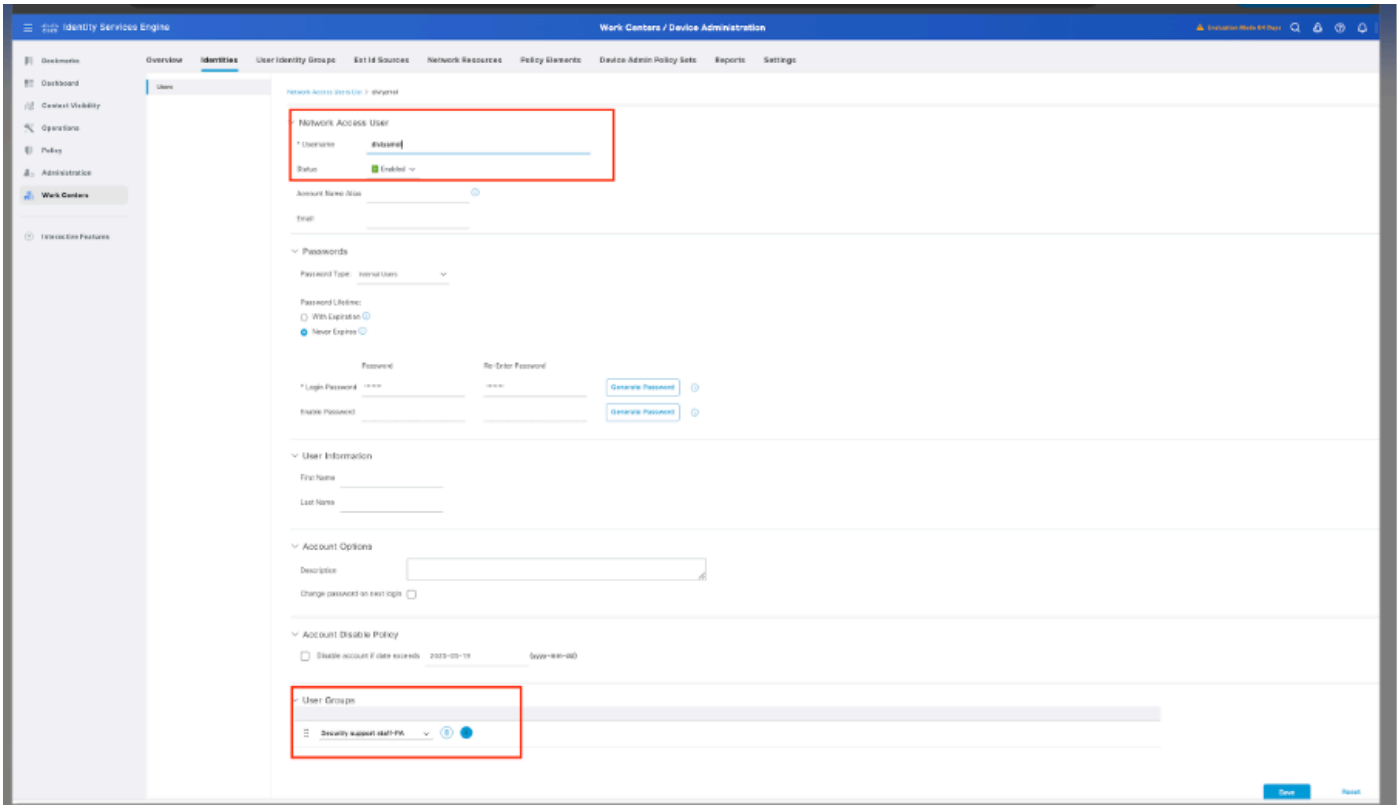
Cliquez sur Save.

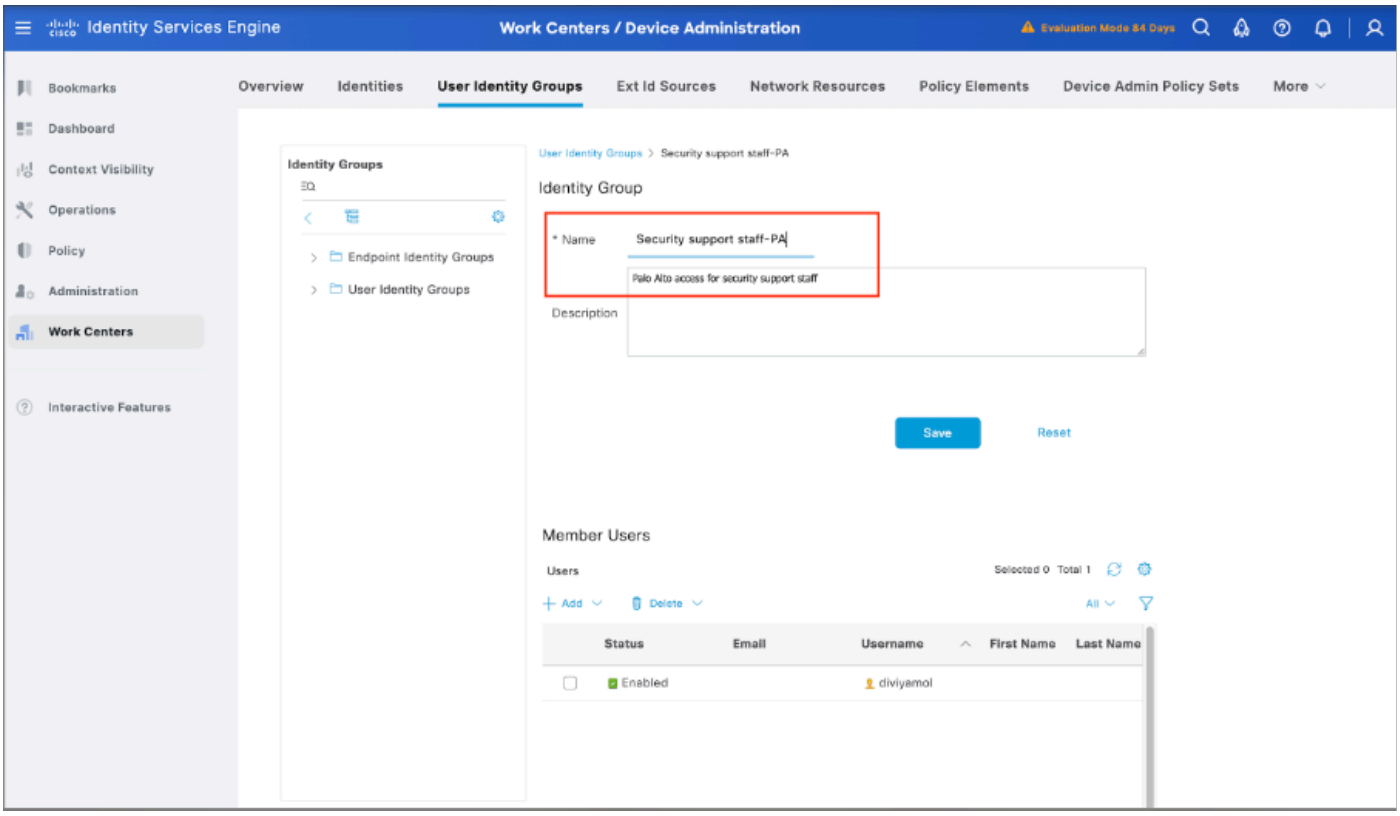


Étape 5 : création de groupes d'identités utilisateur

Accédez à Work Centers > Device Administration > User Identity Groups, puis cliquez sur Add et spécifiez le nom du groupe d'utilisateurs.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

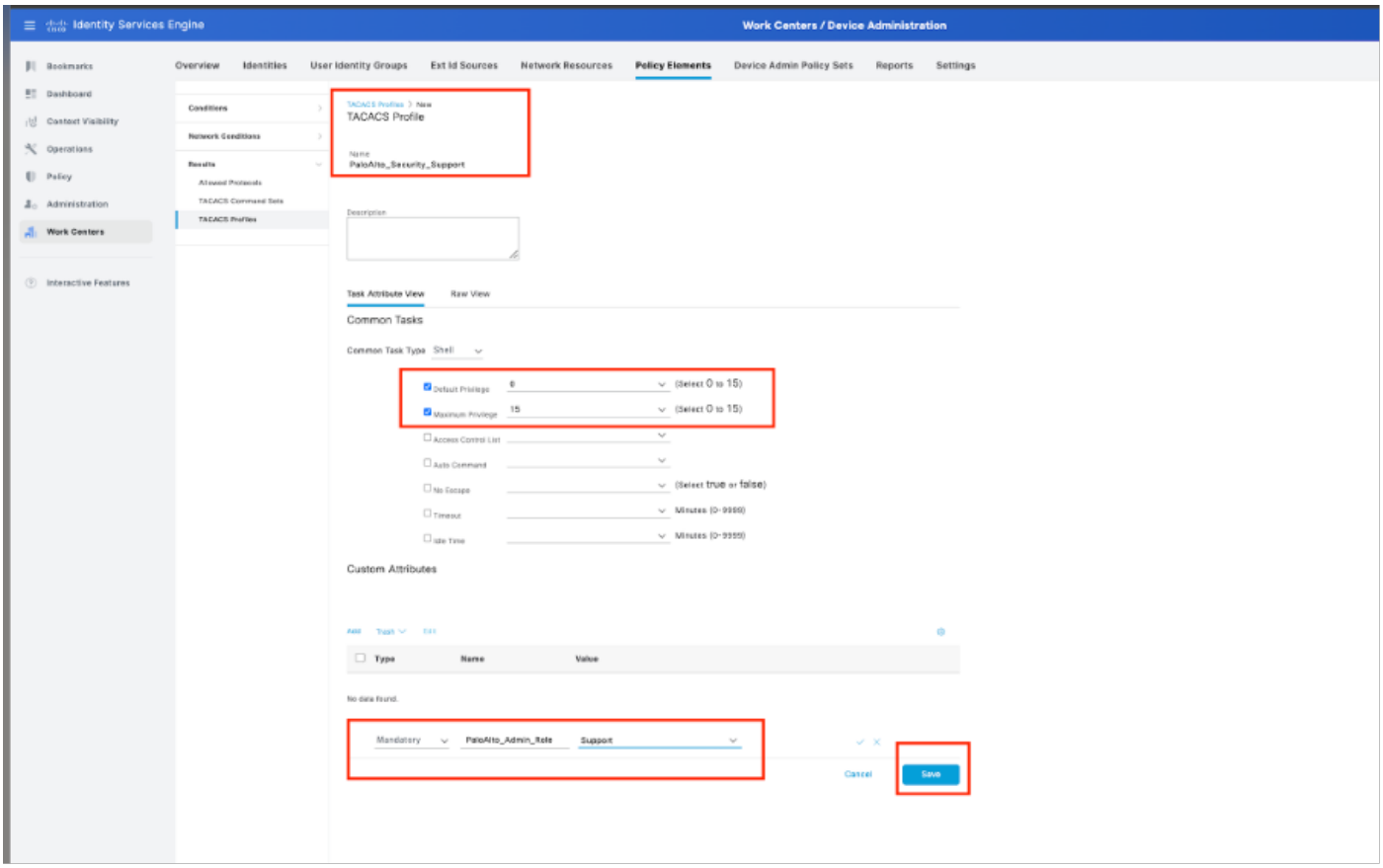


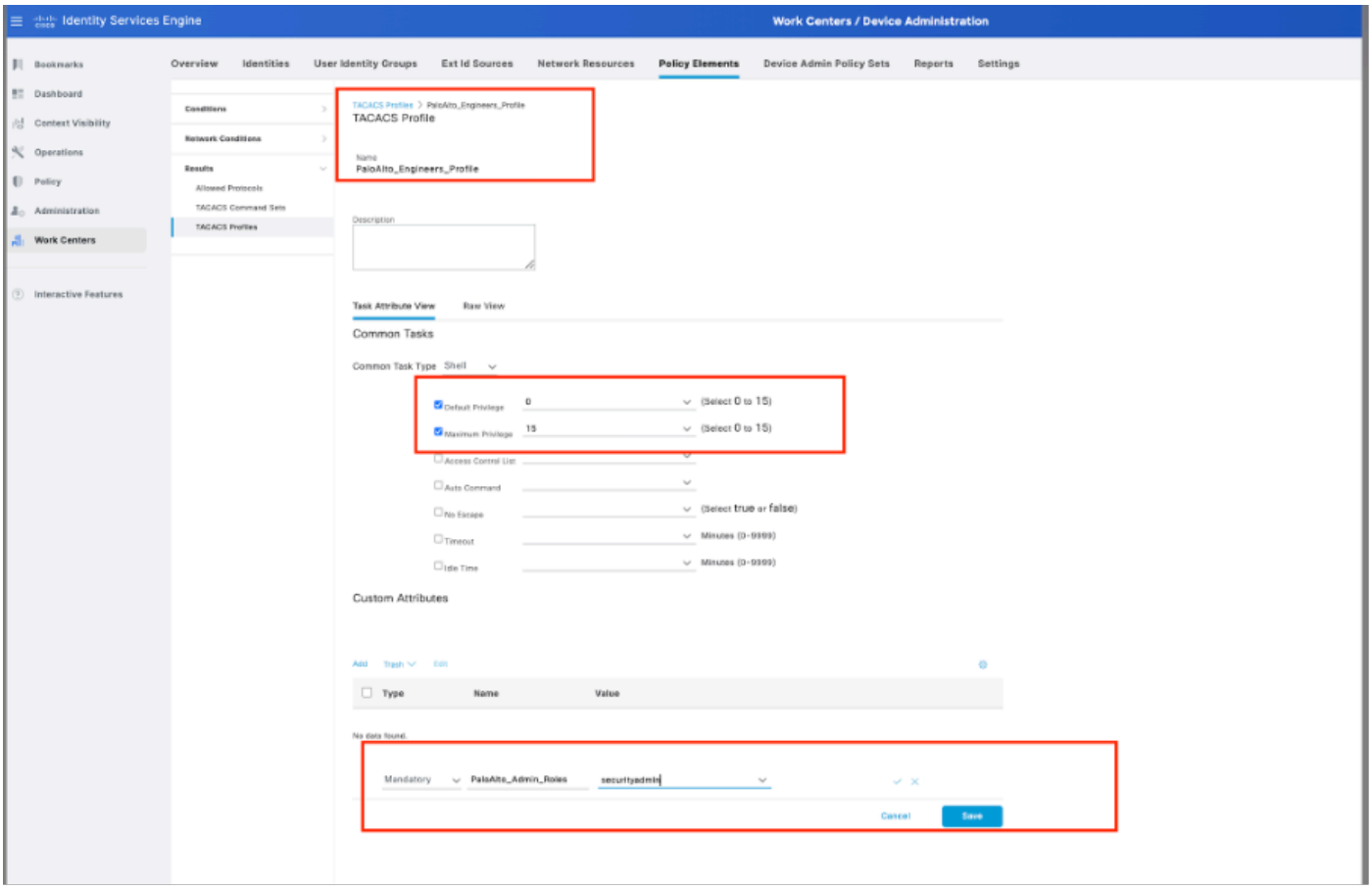


Étape 6 : configuration d’un profil TACACS

Ensuite, vous pouvez configurer un profil TACACS, dans lequel vous pouvez configurer des paramètres tels que le niveau de privilège et le délai d'attente. Accédez à Work Centers > Device Administration -> Policy Elements -> Results -> TACACS Profiles.

Cliquez sur Ajouter pour créer un nouveau profil TACACS. Donnez un nom correct au profil.



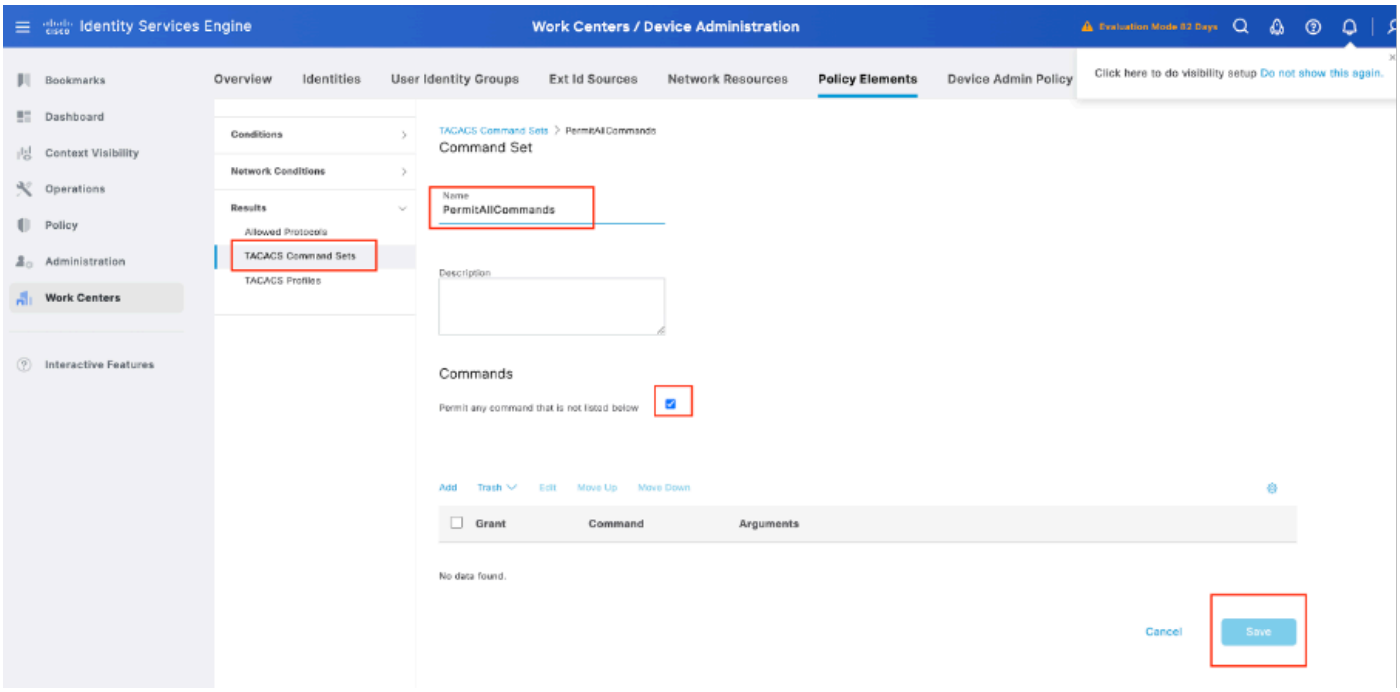


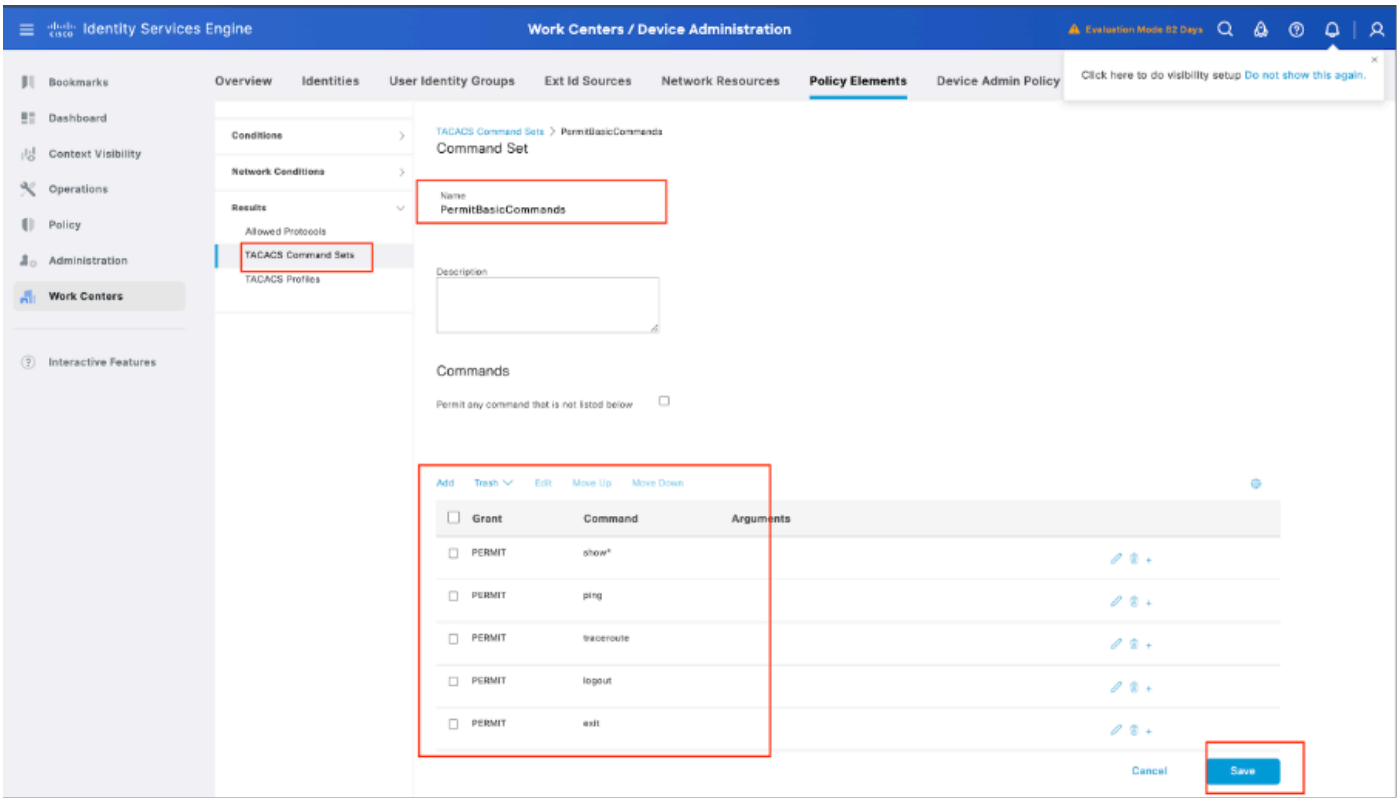
Étape 6 : configuration des jeux de commandes TACACS

À présent, il est temps de configurer les commandes que les utilisateurs sont autorisés à utiliser. Étant donné que vous pouvez accorder à ces deux cas d'utilisation le niveau de privilège 15, qui donne accès à chaque commande disponible, utilisez les jeux de commandes TACACS pour limiter les commandes pouvant être utilisées.

Accédez à Work Centers > Device Administration > Policy Elements > Results -> TACACS Command Sets. Cliquez sur Add pour créer un nouvel ensemble de commandes TACACS et le nommer PermitAllCommands. Appliquez ce jeu de commandes TACACS pour l'assistance à la sécurité.

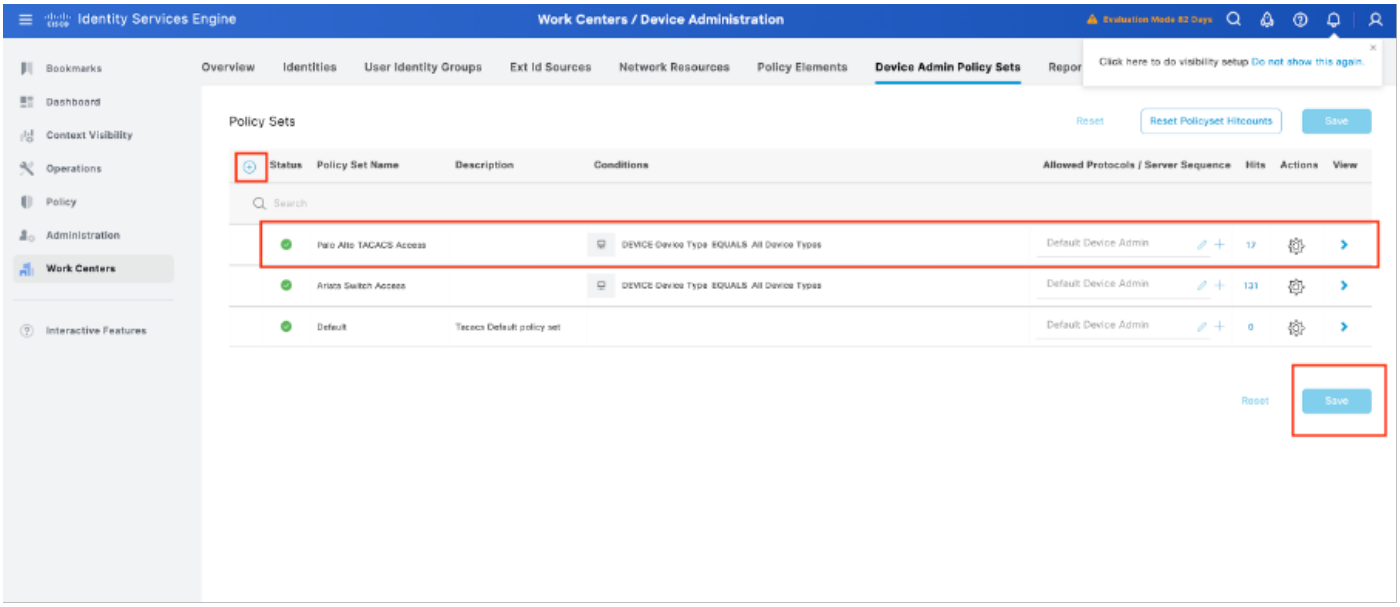
La seule chose que vous devez configurer dans ce jeu de commandes TACACS est de cocher la case Autoriser toute commande qui n'est pas répertoriée ci-dessous.





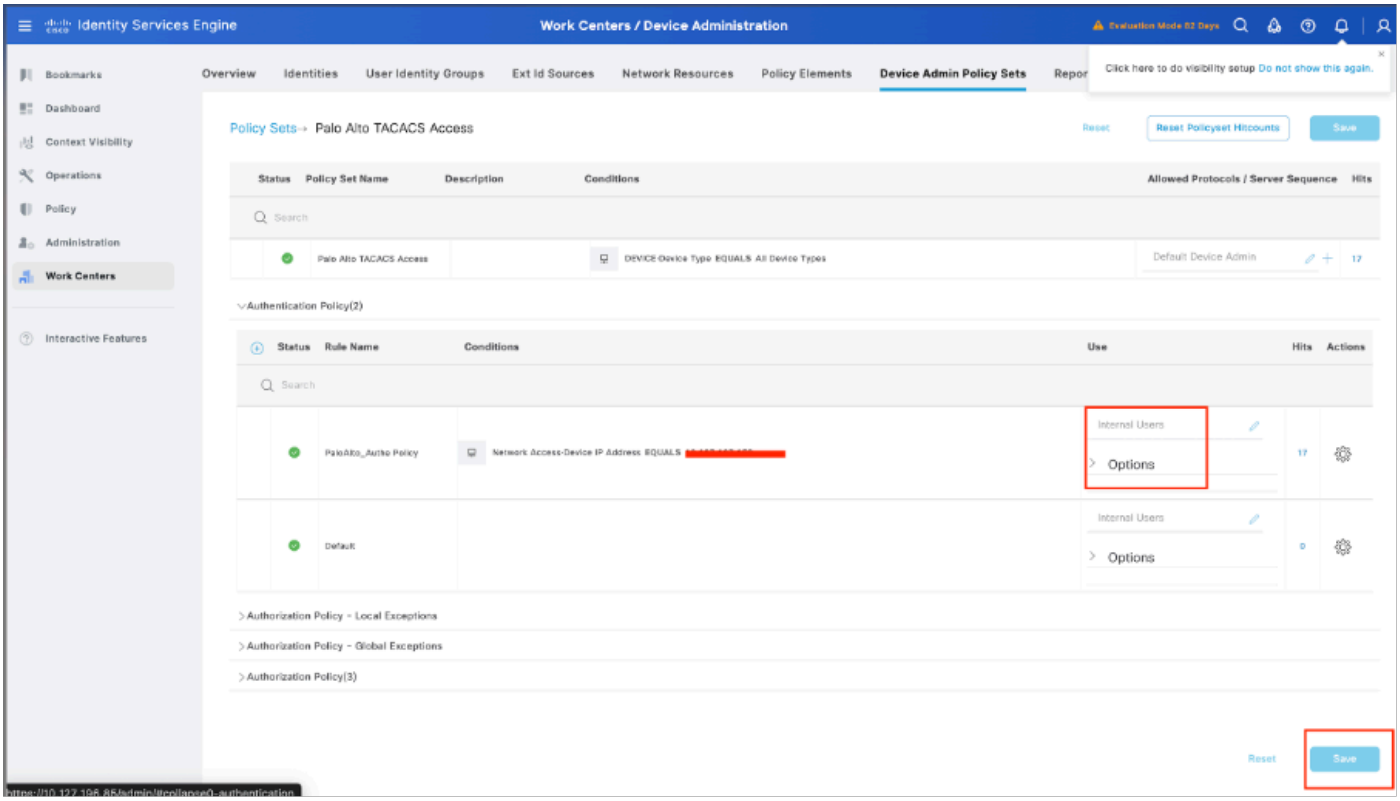
Étape 7. Créez un ensemble de stratégies d'administration de périphériques à utiliser pour votre Palo Alto, accédez au menu Work Centers > Device Administration > Device Admin Policy Sets, cliquez sur l'icône Add +.

Étape 8. Nommez ce nouvel ensemble de stratégies, ajoutez des conditions en fonction des caractéristiques des authentifications TACACS+ en cours à partir du pare-feu Palo Alto et sélectionnez Allowed Protocols > Default Device Admin. Enregistrez votre configuration.

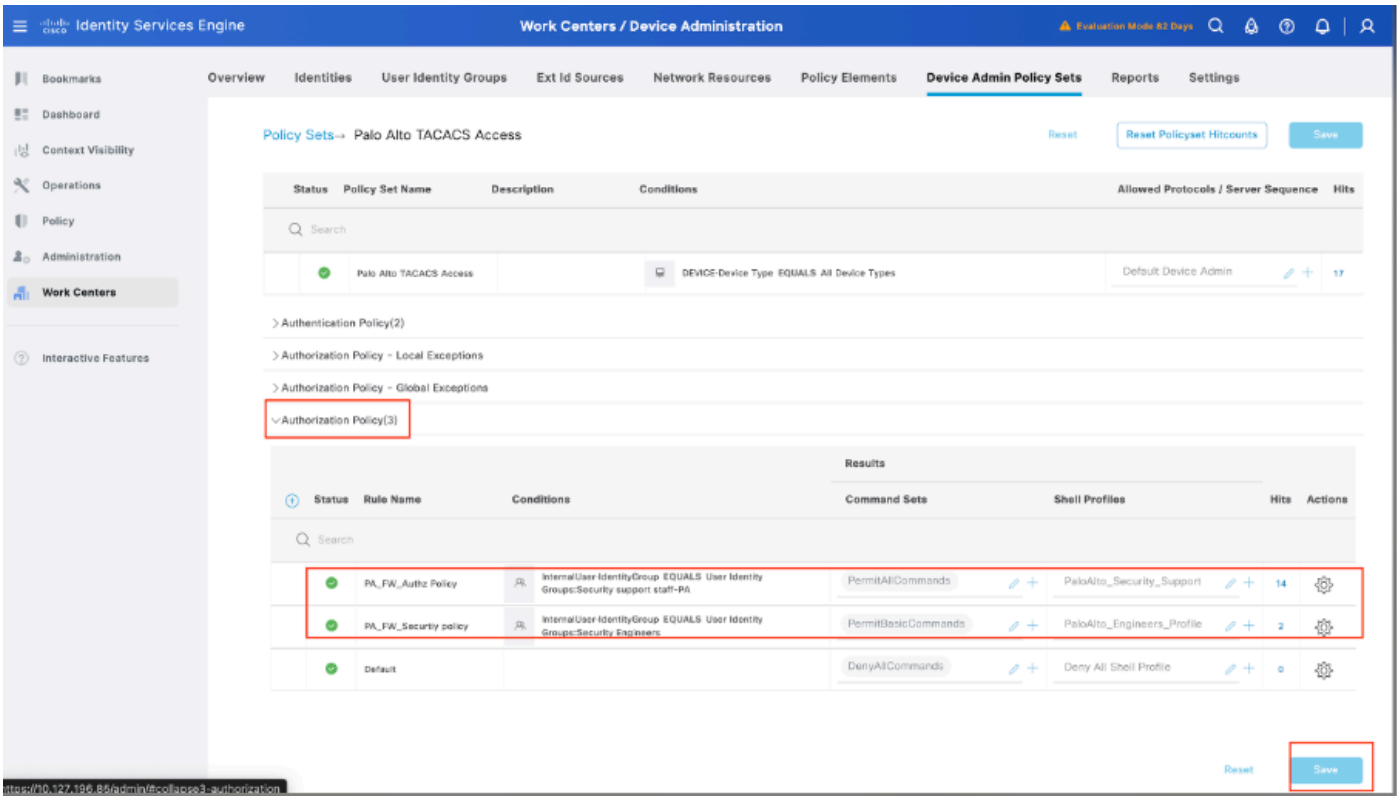


Étape 9. Sélectionnez l'option > view, puis, dans la section Authentication Policy, sélectionnez la

source d’identité externe que Cisco ISE utilise pour interroger le nom d’utilisateur et les informations d’identification pour l’authentification sur le Palo Alto Firewall. Dans cet exemple, les informations d'identification correspondent aux utilisateurs internes stockés dans ISE.



Étape 10. Faites défiler la page jusqu’à la section intitulée Stratégie d’autorisation jusqu’à la stratégie par défaut, sélectionnez l’icône d’engrenage, puis insérez une règle ci-dessus.



Étape 11. Attribuez un nom à la nouvelle règle d'autorisation, ajoutez des conditions concernant l'utilisateur qui est déjà authentifié en tant qu'appartenance à un groupe et, dans la section Profils Shell, ajoutez le profil TACACS que vous avez configuré précédemment, enregistrez la configuration.

Vérifier

Évaluation ISE

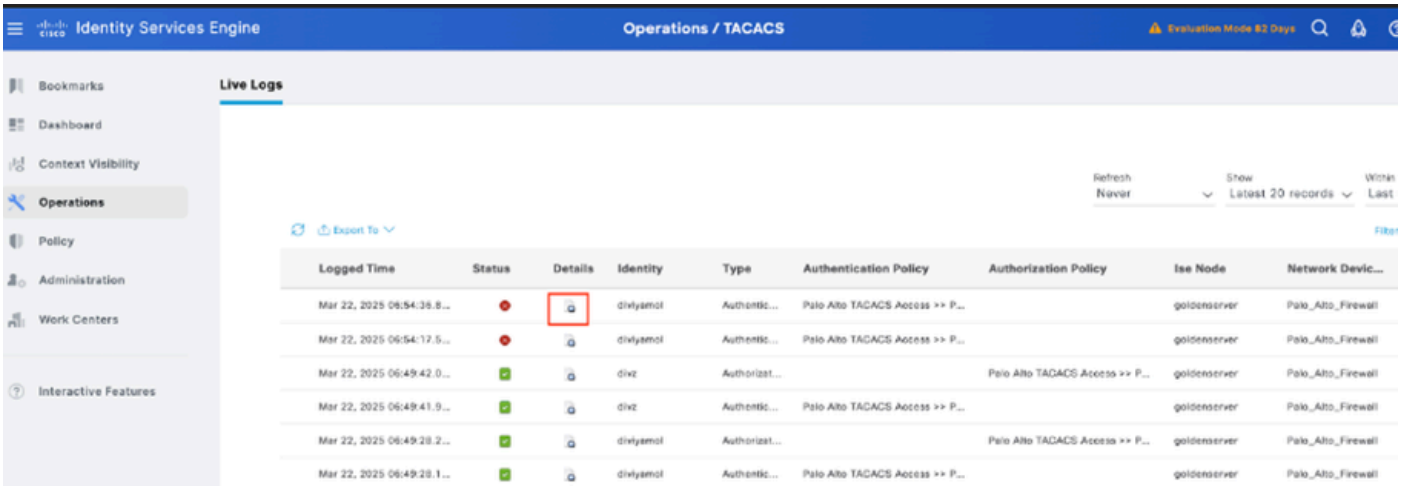
Étape 1. Vérifiez si la facilité de maintenance TACACS+ est en cours d'exécution. Vous pouvez l'intégrer :

- IUG: Vérifiez si le noeud répertorié avec le service DEVICE ADMIN est dans Administration -> System -> Deployment.
- CLI : Exécutez la commande show ports | inclure 49 pour confirmer que le port TCP contient des connexions appartenant à TACACS+

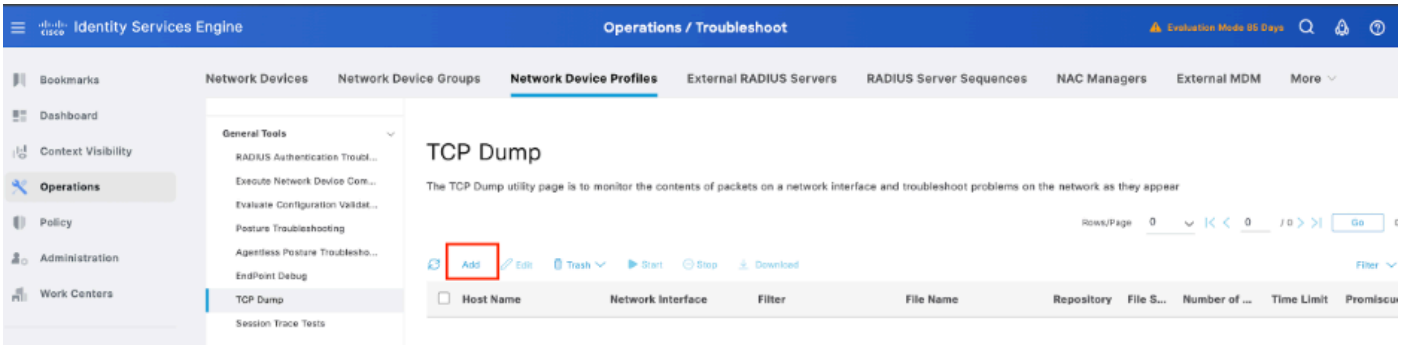
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

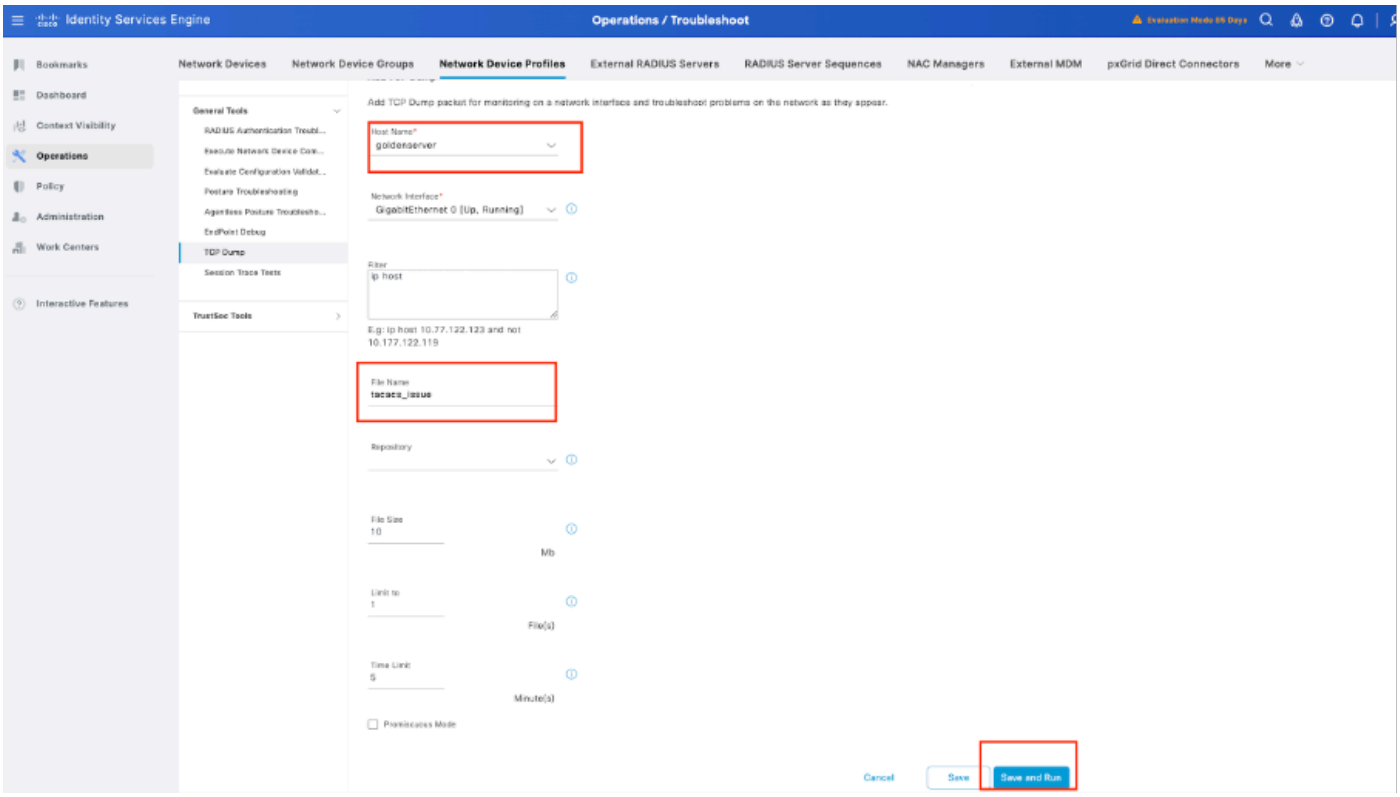
Étape 2. Vérifiez s'il existe des journaux en direct concernant les tentatives d'authentification TACACS+ : vous pouvez le vérifier dans le menu Operations -> TACACS -> Live logs.

En fonction de la raison de l'échec, vous pouvez ajuster votre configuration ou résoudre la cause de l'échec.

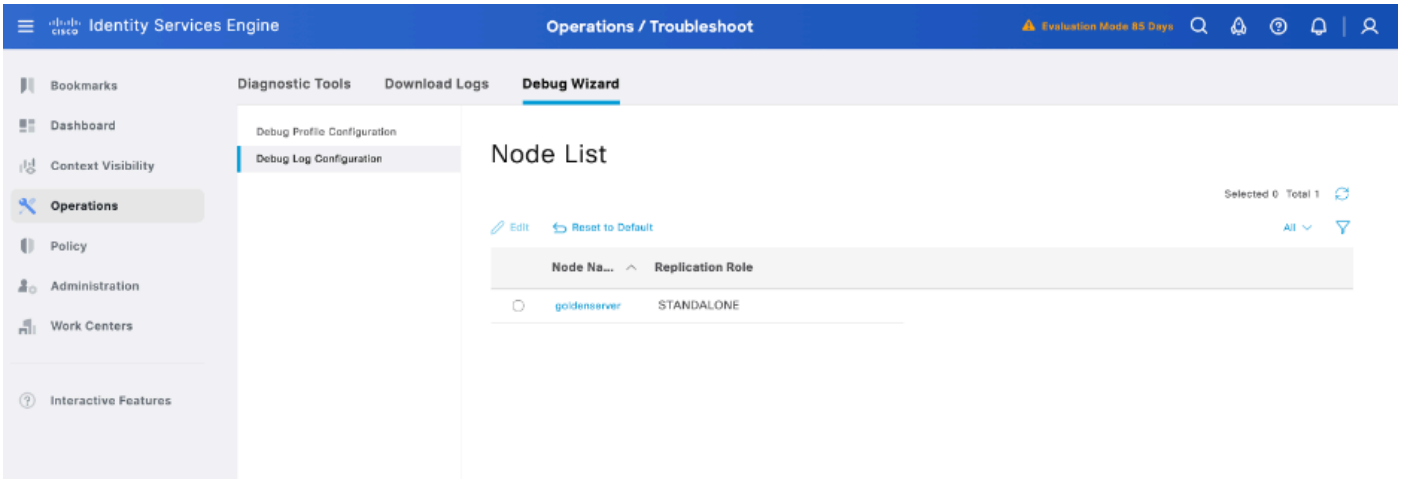


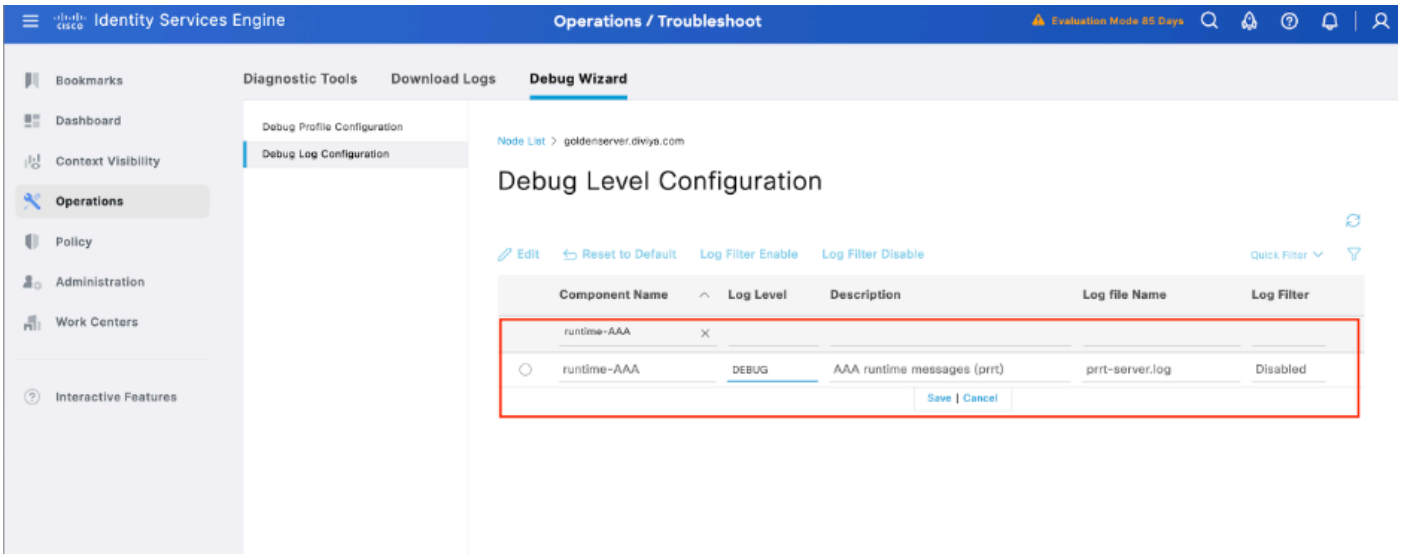
Étape 3. Si vous ne voyez pas de journal en direct, passez à une capture de paquets. Naviguez jusqu'au menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump , sélectionnez Add.





Étape 4. Activez le composant runtime-AAA dans debug dans le PSN à partir de l'endroit où l'authentification est effectuée dans Operations > Troubleshoot > Debug Wizard > Debug log configuration, sélectionnez PSN node , puis next in edit button .





Identifiez le composant runtime-AAA, définissez son niveau de journalisation sur debug, reproduisez le problème et analysez les journaux pour une enquête plus approfondie.

Dépannage

1 TACACS : Paquet de demande TACACS+ non valide - Secrets partagés éventuellement incorrects

Problème

L'authentification TACACS+ entre Cisco ISE et le pare-feu Palo Alto (ou tout périphérique réseau) échoue avec le message d'erreur :
"Paquet de requête TACACS+ non valide - secrets partagés éventuellement non concordants"

Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

Cela empêche les tentatives de connexion d'administration réussies et peut avoir un impact sur le contrôle d'accès au périphérique via une authentification centralisée.

Causes possibles

- Non-concordance dans le secret partagé configuré sur Cisco ISE et le pare-feu Palo Alto ou le périphérique réseau.

- Configuration incorrecte du serveur TACACS+ sur le périphérique (adresse IP, port ou protocole incorrects).

Solution

Il existe plusieurs solutions possibles à ce problème :

1. Vérifiez le secret partagé :

- Sur Cisco ISE :
  Accédez à Administration > Network Resources > Network Devices, sélectionnez le périphérique concerné et confirmez le secret partagé.
- Sur le pare-feu Palo Alto :
  Accédez à Device > Server Profiles > TACACS+ et vérifiez que le secret partagé correspond exactement, y compris la casse et les caractères spéciaux.

2. Vérifiez les paramètres du serveur TACACS+ :

- Vérifiez que l'adresse IP et le port corrects (la valeur par défaut est 49) de Cisco ISE sont configurés dans le profil TACACS+ du pare-feu.
- Vérifiez que le type de protocole est TACACS+ (et non RADIUS).

2.No ISE TACACS Live Log

·Vérifiez le routage/l’interface source du pare-feu et la connectivité TCP/49 au PSN configuré.

·Vérifiez que le pare-feu utilise le nom de domaine complet/IP ISE souhaité.

·Confirmez que le service d'administration des périphériques est activé sur le PSN cible.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.